Cyber tips

GrowthZone webinar follow up

Brian Haney, CLTC, CFBS, CFS, CIS, LACP, CAE

COVID-19 Cyber Security Risks for Remote Association Employees

Thank you for attending the GrowthZone presentation. I hope it provided you with some valuable information and practical steps organizations and individuals can take to remain cyber resilient and protected. We had some excellent questions that I was sadly not able to answer live but wanted to make sure they were answered.

From Michael - " Should I be requiring my staff to install and use a VPN for work at home??" – *Excellent question. Before I answer it, let me begin by describing what a VPN is. A VPN is an encrypted "tunnel" for your online activity that goes through the open internet from your home of. ce or coffee shop to your work network at the office. You can connect across a VPN no matter what network you're on and "appear" as if you were at your office desk at work. The reason it is called a virtual private network is because it creates your own personal channel no one else can access. We highly recommend considering VPN solutions that could fit your organization as they can be a relatively inexpensive way to enhance your protection. If all your team members are working remotely from their home offices, this is how you can work as a virtual team without all being at the main office. Many services provide up to 10 devices per license and most offer the VPN solution for mobile devices in addition to laptops or desktops.*

From Michael - "How vulnerable are apps like Slack" *As far as we can tell Slack and several other messaging apps are fairly secure. By default, Slack encrypts data at rest and data in transit for all of their customers. They also further protect your data with tools like Slack Enterprise Key Management (Slack EKM), audit logs, and integrations with top data loss prevention (DLP) providers. We have several clients using Slack that have shared it is a very good and valuable tool.*

From Dana- " If using a mobile hotspot for WiFi, other than a passcode what are some security protections you can put in place?"

VPN can be a helpful addition to provide further security when using a mobile hotspot. We also encourage increased mindfulness, as most of the cases we have found mobile hotpots in use involve highly trafficked commercial areas (like airports), or at conferences (back when we use to be able to get together in person!). If you're using a hotspot because you want to avoid public wifi, or semi-private wifi in a public setting, we recommend you pay extra careful attention to what you are accessing during that time. While harder to hack, it is not impossible to expose yourself unnecessarily, so be careful not to login to anything (such as a bank account) and perhaps consider not accessing sensitive emails. Best practice is to assume that in a public place, someone can potentially steal whatever it is you're doing, so limit activities to non-sensitive or non-personal data such as social media (if you consider that non sensitive), or using the Starbucks app, reading your news feed, etc...

From Natalie - " What about a password on an airplane to watch entertainment on your devices? Would it be a big risk in the sky if it is not password protected?" *Natalie, accessing news and entertainment on an airplane is generally okay, especially since most airlines require you to login through their app and they limit what you can access and it's usually one-way content distribution (meaning you're not sending out data, they are just streaming it to you). When it becomes risky is when you use the plane's wifi network to do work on your laptop or mobile device because then it's no different than a coffee shop. There are some that decide to do work without logging in or accessing a network, and while that is certainly better than exposing data over a network connection, you still want to be careful what's on your screen and who can see it on the plane. The cameras in most smartphones can be pretty powerful and it wouldn't be hard for someone to snap pictures without you knowing it.*

From Len: "What type of tools do you use or recommend to store the 10,000 passwords we need to keep track of?" *Len, I have to admit that for me, password management is the worst part of being cyber vigilant because I just don't have the bandwidth. To that end there are many viable programs and apps that can help. Norton Antivirus has a password manager solution as do many Antivirus providers, and there are many quality vendors that can help you with everything from securely saving your passwords so you don't forget them, to autogenerating ones so you don't have to constantly pick different crazy versions of current ones. I'd go with a program you feel fits your needs best, since some have more robust passwords needs than others.*

Closing thoughts

Now is the best time for a comprehensive insurance audit. Make sure your policies cover remote work and employees using personal devices. Work with an insurance professional that understands the association industry and can help create a roadmap for organizational risk management moving forward.

Properly designed insurance coverage is really the intersection of two critical elements of protection. The first and possibly more essential factor is an organization's own risk assessment. Make sure you have policies covering information and data security and make sure your IT infrastructure supports those policies. Understand how the vendors you work with support privacy. Only by seeing your operational and human capital risks and developing the right policies and procedures can you properly transfer certain exposures to an insurance company through a policy. Use this crisis as an opportunity to examine and refine your operational policies and procedures to better address current and future risks.

Practice good cyber hygiene and be proactive when you hear about new or evolving risks or adopt new technology and incorporate it into your association. Plan, prepare, adjust, and prosper!

We are 2 CAE's on a Mission to help you be Cyberific!

When an Association industry veteran who is both an ASAE Fellow and a CAE gets together with a tech savvy and somewhat edgy financial professional who is also a CAE, good things happen. Never hurts if those two happen to be father and son!

Allen Haney was the first broker to receive the ASAE All Star Award in Insurance & Financial Services. Highly respected in the Association and Non-profit community for his ability to solve problems.

Brian Haney is a 16-year financial professional experienced in banking, employee benefits, retirement plans, and insurance with expertise in both the non-profit and for-profit markets. A self-avowed tech junky, he runs the "That's My Financial Guy Podcast" and has been awarded as one of NAIFA's 4 UNDER 40, The Washington Business Journal's 40 UNDER 40, and was NAIFA's Diversity Champion in 2018.

As the only financial services firm owned and operated by not one, but two Certified Association Executives, The Haney Company offers Associations solutions and advice with the assurance that we don't just understand financial services & insurance, but share a unique understanding of Associations and the day-to-day challenges Association professionals face. WE ARE TWO CAEs ON A MISSION!

The Haney Company

Insurance and Financial Services